Commonwealth Office of Technology Monthly Cyber Security Tips

JUNE 2006 Volume 1, Issue 1

Why Cyber Security is Important

From the Desk of the Chief Information Security Officer

What is cyber security?

It seems that everything relies on computers and the Internet now — communication (email, cell phones), entertainment (digital cable, MP3's), transportation (car engine systems, airplane navigation), shopping (online stores, credit cards), medicine (equipment, medical records), and the list goes on. How much of your daily life relies on computers? How much of your personal information is stored either on your own computer or on someone else's system?

Cyber security involves protecting that information by preventing, detecting, and responding to attacks.

What are the risks?

There are many risks, some more serious than others. Among these dangers are viruses erasing your entire system, someone breaking into your system and altering files, someone using your computer to attack others, or someone stealing your credit card information and making unauthorized purchases. Unfortunately, there's no 100% guarantee that even with the best precautions some of these things won't happen to you, but there are steps you can take to minimize the chances.

What can you do?

The first step in protecting yourself is to recognize the risks and become familiar with some of the terminology associated with them.
Hacker, attacker, or intruder - These terms are applied to the people who seek to exploit weaknesses in software and computer systems for their own gain. Although their intentions are sometimes fairly benign and motivated solely by curiosity, their actions are typically in violation of the intended use of the systems they are trying to exploit. The results can range from mere mischief (creating a virus with no intentionally negative impact) to malicious (stealing or altering information).

Malicious code - This category includes computer code such as viruses, worms, and Trojan horses. Although some people use these terms interchangeably, they have unique characteristics.

- **Viruses** - This type of malicious code requires you to actually do something before it infects your computer. This action could be opening an email attachment or going to a particular web page.
- **Worms** - Worms propagate without user intervention. They typically start by exploiting a software vulnerability (a flaw that allows the software's intended security policy to be violated), then once the victim computer has been infected the worm will attempt to find and infect other computers. Similar to viruses, worms can propagate via email, web sites, or network-based software. The automated self-propagation of worms distinguishes them from viruses.

Trojan horses - A Trojan horse program is software that claims to be one thing while in fact doing something different behind the scenes. For example, a program that claims it will speed up your computer may actually be sending confidential information to a remote intruder.

This series of information security tips will give you more information about how to recognize and protect yourself from attacks.

For more information and this and other topics please visit the Commonwealth Office of Technology's Website at http://technology.ky.gov/security/cyber_security.htm

Brought to you by: MS-ISAC ***Powered by:*** US-CERT UNITED STATES COMPUTER EMERGENCY READINESS TEAM

http://www.msisac.org

http://technology.ky.gov/